

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-161880  
(43)Date of publication of application : 19.06.1998

(51)Int.Cl. G06F 9/445  
G06F 13/00  
H04L 9/32  
H04L 12/46  
H04L 12/28

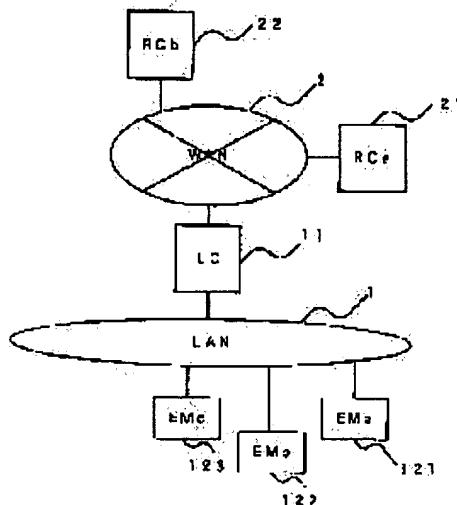
(21)Application number : 08-319074 (71)Applicant : HITACHI LTD  
(22)Date of filing : 29.11.1996 (72)Inventor : EBATA TOMOKAZU ORIMO MASAYUKI

**(54) REMOTE CONTROL SYSTEM**

(57)Abstract:

**PROBLEM TO BE SOLVED:** To control an object device connected to a local area network via a local or remote controller.

**SOLUTION:** When the devices 121 to 123 to be controlled are connected to a network 1, a control program of its own is installed in a local controller 11 which controls the devices 121 to 123 by means of the installed control program. When the control program is installed, the controller 11 registers the detailed information on the devices 121 to 123 in the remote controllers 21 and 22. When the version up is performed for the control program, the controllers 21 and 22 install the control program in the controller 11.



## **LEGAL STATUS**

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-161880

(43)公開日 平成10年(1998)6月19日

(51)Int.Cl.<sup>6</sup>  
G 0 6 F 9/445  
13/00 3 5 1  
H 0 4 L 9/32  
12/46  
12/28

F I  
G 0 6 F 9/06  
13/00 3 5 1 H  
H 0 4 L 9/00  
11/00 6 7 3 B  
3 1 0 C

審査請求 未請求 請求項の数 6 O L (全 15 頁)

(21)出願番号 特願平8-319074

(22)出願日 平成8年(1996)11月29日

(71)出願人 000005108  
株式会社日立製作所  
東京都千代田区神田駿河台四丁目6番地

(72)発明者 江端 智一  
神奈川県川崎市麻生区王禅寺1099番地株式  
会社日立製作所システム開発研究所内

(73)発明者 織茂 昌之  
神奈川県川崎市麻生区王禅寺1099番地株式  
会社日立製作所システム開発研究所内

(74)代理人 弁理士 小川 勝男

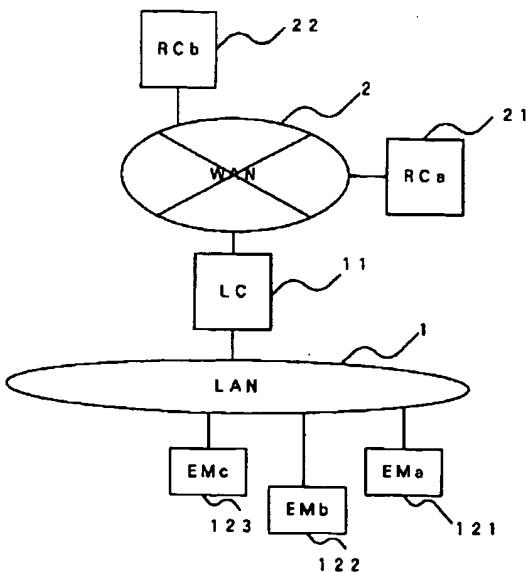
(54)【発明の名称】 リモート制御方式

(57)【要約】

【課題】ローカルエリアネットワークに接続された被制御装置を、ローカルコントローラあるいはリモートコントローラから制御する。

【解決手段】被制御装置がネットワークに接続するときに、自分を制御する制御プログラムをローカルコントローラにインストールし、ローカルコントローラはインストールされた制御プログラムで被制御装置の制御を行う。また、制御プログラムがインストールされた時点で、ローカルコントローラは、リモートコントローラに被制御装置の詳細な情報を登録する。リモートコントローラは、制御プログラムのバージョンアップが行われた時に、バージョンアップされた制御プログラムをローカルコントローラにインストールする。

図 1



## 【特許請求の範囲】

【請求項1】ローカルエリアネットワークで接続された少なくとも一つ以上の制御を管理するローカル制御装置とローカル制御装置によって制御される少なくとも一つ以上の被制御装置と、ワイドエリアネットワークで接続される少なくとも一つ以上のリモートに配置されたリモート制御装置から構成されるシステムにおいて、上記被制御装置が自装置を制御する制御プログラムを、上記ローカル制御装置にインストールすることを特徴とするリモート制御方式。

【請求項2】請求項1において、上記ローカル制御装置が上記被制御装置を制御する制御プログラムを、上記リモート制御装置からインストールするリモート制御方式。

【請求項3】請求項1において、上記被制御装置がその装置の情報を上記ローカル制御装置に送信し、上記ローカル制御装置がその情報と上記制御プログラムを用いて制御情報を生成し、生成した制御情報を上記被制御装置に送信することによって、上記被制御装置を制御するリモート制御方式。

【請求項4】請求項1において、上記リモート制御装置あるいはシステム外部の装置が上記ローカル制御装置にメッセージを送信し、そのメッセージに従って上記ローカル制御装置が上記被制御装置を制御するリモート制御方式。

【請求項5】請求項1において、上記被制御装置から送信されたメッセージに対し、上記ローカル制御装置がそのメッセージ内容を解析し、予め定められた上記リモート制御装置あるいはシステムの外部の装置にメッセージを送信するリモート制御方式。

【請求項6】請求項1において、メッセージおよび制御プログラムの送信を行うときに、送信元の装置を認証する電子認証を付加し、暗号処理を施した情報を送信するリモート制御方式。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明はリモート制御システムに関する。

## 【0002】

## 【従来の技術】

(1) 現在の家電製品および自動車の制御部の殆どにはマイコンが搭載されている。これらの製品は、ROMに書き込まれた制御プログラムに従って制御が行われるため、従来のマイコンが搭載されていない製品に比べ、高度な制御が可能となってきている。マイコンのハードの基本性能が変わらなくても、プログラムを改良していくことによって、新製品は制御の精度を向上させることができとなり、多様な条件下での制御が行えるようになってきている。

## 【0003】(2) 例えば、日経コミュニケーション N 50

o. 226(1996年7月)によると、ネットワークコンピュータ(以下、NCと略す)とネットワークで構成されるシステムは以下の特徴を持っている。

【0004】(a) アプリケーションプログラムのインストール、OSのバージョンアップを各クライアント装置に別々に施す必要がなく、ネットワークに繋がっている管理サーバに行わせることによって、常にシステムを構成する装置に最新のバージョンを一斉にインストールすることが可能である。

10 【0005】(b) 制御管理サーバ上でのソフトウェアの一元管理や運用管理を容易に実現できるため、不正コピーの防止、システムの一斉切り替えなどにおいて、運用管理の工程が削減できる。

【0006】このようにNCでは、ネットワークに繋がった各クライアント装置の管理を制御管理サーバに集中させることができる一方で、処理は分散の形態を維持することが可能となる。

【0007】(3) 例えば、OPEN DESIGN No. 8 電子メールシステム完全マスタCQ出版社によると、PCのオペレーティングシステムであるWindows NTのPCネットワーク環境は、

(a) LAN Manager 環境

(b) NetWare 環境

(c) Macintosh 環境

(d) 非同期接続

に大別される。(a)では、ドメイン管理機能、ユーザ管理機能、ドメインの信頼関係構築機能、セキュリティモデル構築機能、ファイル共有機能、プリンタ管理機能、ネットワークアプリケーション環境機能がある。

30 (b)では、IPX/SPX互換トランスポrt機能の他に、クライアントソフトウェア機能、ゲートウェイ機能が標準で提供される。(c)では、Macintosh クライアントへのファイル共有機能、プリンタ共有機能、AppleTalk ネットワークプリンタの利用機能などがある。(d)では、RAS、PPP/SLI P、TCP/IPツールなどがある。

【0008】この様にWindows NTでは、マルチプロトコルを扱うことが出来るため、マルチベンダの機器からなるオープン環境下で、ネットワーク機能を利用したパソコンLANの構築や管理が容易である。

## 【0009】

【発明が解決しようとする課題】上記の方式では、次に示す問題が発生する。

【0010】(1) の方式では、家電製品に内蔵する必要性とコストの問題から、小型でかつ低機能のマイコンと、新規に書き込みができないようなプログラム読み出し専用のメモリ(ROM)を使用している。このため、一般にこれらの製品では、製品を購入した後で、制御プログラムのバージョンを上げて制御性能を上げることは出来ないし、使用者の要求に従って制御方式をカスタマ

イズすることも出来ない。

【0011】また(1)の方式では、低機能・低クロックのマイコンを用いているため、製品のセンサ情報を使って精密な制御を行うことが困難であると言う問題がある。

【0012】本発明では、これらの家電製品をローカルエリアネットワークで結び、家電製品が自分の制御に必要となる制御プログラムをローカルエリアネットワークに繋がったローカル制御装置にインストールし、ローカル制御装置から家電製品などの被制御装置を制御することで上記問題を解決する。

【0013】さらに本発明では、家電製品などの被制御装置の製造元メーカーが、制御プログラムのバージョンアップを行ったり、リモートメンテナンス等を行うリモート制御装置を供え、これを前記のローカル制御装置とワイドエリアネットワークで接続する事によって、ローカル制御装置が被制御装置を制御する制御プログラムを、リモート制御装置からインストールすることで上記問題を解決する。

【0014】また(1)の方式では、製品が複数の制御方式を持つようになりユーザがその制御方式を選択できるようになるのに従い、それに伴って制御を選択するマンマシンインターフェースが複雑になってくる。この為、ユーザは製品に付加する多数の高機能制御を十分に使いきれないと言う問題が発生する。

【0015】また(1)の方式では、製品の定期的なメンテナンスを行うことができず、ユーザが製品の異常や停止になった時点で、初めて故障に気がつくと言う問題がある。

【0016】本発明では、リモート制御装置あるいはシステム外部の装置がローカル制御装置にメッセージを送信し、そのメッセージに従ってローカル制御装置が被制御装置を制御することや、家電製品などの被制御装置から送信されたメッセージに対し、ローカル制御装置がそのメッセージ内容を解析し、予め定められたリモート制御装置あるいはシステムの外部の装置にメッセージを送信することで、上記の問題を解決する。

【0017】さらに、家電製品などの被制御装置をローカルエリアネットワークで結び、家電製品が自分の制御に必要となる制御プログラムをローカルエリアネットワークに繋がったローカル制御装置にインストールすることで、次のような課題を解決することができる。

【0018】例えば(2)の方式で管理サーバがクライアント装置の制御を行う場合には、OSやアプリケーションのインストールを管理サーバに管理させるため、サーバは様々な種類のOSやアプリケーションを常に管理しておく必要があり、管理サーバの負荷が高くなるし、また、クライアント装置は起動時(電源投下時)にOSやアプリケーションのプログラムをインストールしてから起動するため、伝送帯域が十分でない場合は、ネット

ワークトラヒックの負荷が高くなると言う問題があるが、本発明の方式では、被制御装置が予め自分の内部装置に自分自身を制御するプログラムを所有し、システムに参入する時点でリモート制御装置に制御プログラムをインストールするので、この様な問題は発生しない。

【0019】また(2)(3)の方式では、管理サーバとクライアント装置の間で制御情報などのメッセージをやりとりする場合に、その装置がメッセージを送受信する権利を持つ装置であるかどうかを認識する手段がない。また、ある装置が正規の装置になりすまして、不当にメッセージの送受信を行う場合、それを妨げる手段がないし、メッセージが盗聴されていた場合、情報の秘密を守る手段がない。

【0020】本発明では、メッセージおよび制御プログラムの送信を行うときに、送信元の装置を認証する電子認証を付加し、暗号処理を施した情報を送信することで上記の問題を解決する。

#### 【0021】

【課題を解決するための手段】本発明のリモート制御方式は、(a)ローカルエリアネットワーク(以下LANと略す)及びワイドエリアネットワーク(以下、WANと略す)に繋がるローカル制御装置、(b)LANにつながりローカル制御装置に制御される被制御装置、

(c)WANに接続され前記ローカル制御装置と通信を行うリモート制御装置、(d)リモート環境で通信を行うことが可能な移動体端末装置、に、以下の手段を設定することにより達成できる。すなわち、

(1)被制御装置が、被制御装置の必要とする制御プログラムをローカル制御装置にインストールする手段。

【0022】(2)リモート制御装置が、被制御装置の必要とする制御プログラムをローカル制御装置インストールする手段。

【0023】(3)被制御装置とローカル制御装置間、及びローカル制御装置とリモート制御装置間、及びローカル制御装置と移動体端末間でメッセージの送受信を行う手段。

【0024】(4)それぞれの装置が、送信するメッセージを暗号化し、自装置を認証するために電子署名をメッセージに付加し、その暗号化したメッセージを復号化し電子認証を行う手段。

#### 【0025】

#### 【発明の実施の形態】

(実施例1)図1は実施例1で、本発明が適用されるシステムの全体構成を示す図である。

【0026】図1で、1はローカルネットワーク(以下、LANと呼ぶ)であり、11はLAN1に接続された各装置を制御するローカルコントローラ(以下、LCと呼ぶ)であり、その内部のメモリにプログラムを格納し、これを実行することが可能である。LAN1は、任意のネットワークを構成する伝送媒体による任意の形態

のローカルエリアネットワークで良い。121、122、123は、LAN1に接続し、LC11によって制御される制御対象（以下、EMと略す）であり、その内部のメモリにプログラムを格納し、これを実行することが可能であり、LC11やその他のEMとの通信を行うことも可能である。

【0027】2はワイドエリアネットワーク（以下、WANと呼ぶ）であり、WAN2は、任意のネットワークを構成する伝送媒体による任意の形態のワイドエリアネットワークで良い。21、22はWAN2に接続され、同じくWAN2に接続されたLC11との間で通信や制御を行いうリモートコントローラ（以下、RCと略す）である。RCa21、RCb22は、その内部のメモリにプログラムを格納し、これを実行することが可能である。

【0028】図2は、図1のローカルコントローラLC11の説明図である。111は、通信の管理を司るプロトコルを有する通信管理モジュールである。このモジュールは、LC11が使用する通信インターフェース及びプロトコルにあわせて複数あっても良い。この通信管理モジュール111は、通信メッセージの送受信を司り、メッセージの送達保証や必要に応じて伝送帯域の確保などを行う。112は、通信メッセージの暗号、復号、及び電子認証を行う暗号モジュールである。暗号モジュール112では、受信したメッセージを復号化し、さらにメッセージ内部に記載されている電子署名を確認して、メッセージの送信元が確かにシステムを構成する装置であるかを確認する。この様に復号化されたメッセージはメッセージヘッダの識別コードを読み込んで、メッセージの種類が制御プログラムであるか、あるいはセンサ情報や制御情報であるかを判別する。113は、プログラム転送エージェント（以下、PTAと呼ぶ）であり、ファイル転送プロトコルを用いてプログラムを転送する。PTA113は、制御プログラム（以下、CPと呼ぶ）の送受信、CPの格納、登録、登録削除、CPの起動、及び停止を司る。114は、メッセージ転送エージェント（以下、MTAと呼ぶ）であり、センサ情報や制御情報の管理を司る。MTA114は、暗号モジュール112から送られてきたメッセージを解析し、メッセージからデータを抽出した後、これを一時的に内部に格納し、所定のタイミングでCPに転送する。またCPから受け取ったデータを、一時的にその内部に格納し、転送先等の情報を付加したヘッダ部を持つメッセージにデータを組み込み、所定のタイミングで暗号モジュール112に送出する。CP115は、PTA113によって起動されたCPの一つであり、このCPがネットワークを介して接続されたEMの制御を司る。MTA114から送られてきたあるEMのセンサ情報の内容を解析・計算し、得られた制御情報をEMに送信する。または遠隔地にあるRCにセンサ情報を転送し、RCから送信された制御

情報をEMに転送する。また、CPはユーザがEMの状態を検知できるように、状態を表示したり、ユーザからの制御要求を受け付けることの出来るユーザインターフェースを提供する。あるいは、ユーザインターフェースモジュール116との間でデータをやりとりして、ユーザに制御状態を示したり、ユーザからの制御要求を受け付けることを可能とする。CPは制御するEMのそれぞれに対して用意されるが、CPとEMの関係はかならず1対1でなくても良い。

10 【0029】上記の装置は、ハードウェア、ソフトウェアいずれの方法で実現されても良いし、両者を組み合わせて実現しても良い。

【0030】図3は、図1の制御対象EMa121の内部構成を示す図である。EMa121は、通信モジュール部1211と制御対象の本体部1212に分かれる。

【0031】12111は、通信の管理を司るプロトコルを有する通信管理モジュールである。この通信管理モジュール12111は、通信メッセージの送受信を司り、メッセージの送達保証や必要に応じて伝送帯域の確保などを行う。12112は、通信メッセージの暗号、復号、及び電子認証を行う暗号モジュールである。暗号モジュール12112では、受信したメッセージを復号化し、さらにメッセージ内部に記載されている電子署名を確認し、送信元が確かにシステムを構成する装置であるかを確認する。12113は、ファイル転送プロトコルを用いてプログラムを転送するPTAである。PTA12113は、自EMが接続されているLAN1のLCに自EMを制御するCPを転送する機能を持つ。12114は、センサ情報や制御情報の管理を司るMTAである。MTA12114は、暗号モジュール12112から送られてきたメッセージを解析し、メッセージからデータを抽出した後、これを一時的に内部に格納し、所定のタイミングでデータインターフェース12116と制御対象の本体部1212のデータインターフェース1212を介して、本体12121との間でセンサ情報や制御情報の通信を行う。

【0032】上記の装置は、ハードウェア、ソフトウェアいずれの方法で実現されても良いし、両者を組み合わせて実現しても良い。

40 【0033】図4は、図1のリモートコントローラRC21の説明図である。211は、通信の管理を司るプロトコルを有する通信管理モジュールである。このソフトウェアは、RC21が使用する通信インターフェース及びプロトコルに併せ、複数あっても良い。この通信管理モジュール211は、通信メッセージの送受信を司り、メッセージの送達保証や必要に応じて伝送帯域の確保などをを行う。212は、通信メッセージの暗号、復号、及び電子認証を行う暗号モジュールである。暗号モジュール212では、受信したメッセージを復号化し、さらにメッセージ内部に記載されている電子署名を確認し、送

信元が確かにシステムを構成する装置であるかを確認する。この様に復号化されたメッセージは、メッセージの種類がCPであるか、あるいはセンサ情報や制御情報であるかは、メッセージヘッダの識別コードを読み込んで判別する。PTA213は、CPの送受信、CPの格納、登録、登録削除、プログラムの起動、及び停止を司る。この他、新しいバージョンや変更されたCPなどを格納して、予め登録されたLCにCPのインストールを行う。MTA214は、暗号モジュール212から送られてきたメッセージを解析し、メッセージからデータを抽出した後、これを一時的に内部に格納し、所定のタイミングでCP215に転送する。またCP215から受け取ったデータを一時的にその内部に格納し、転送先等の情報を付加したヘッダ部を持つメッセージにデータを組み込み、所定のタイミングで暗号モジュール212に送出する。CP215は、PTA213によって起動されたCPであり、ローカルコントローラから送られてきたメッセージを、通信管理モジュール211、暗号モジュール212、MTA214を介してデータを受信し、所定の処理を行った後、前述の経路を逆に経由してローカルコントローラへデータを送信する。また、RC21を使用するユーザが制御の状態を検知できるように制御状態を表示し、ユーザからの制御要求を受け付けることの出来るユーザインターフェースを提供する。あるいは、ユーザインターフェースモジュール216との間でデータをやりとりして、ユーザに制御状態を示したり、ユーザからの制御要求を受け付けることができる。CPは制御するLAN1のEMに対して用意されるが、CPとEMの関係はかならず1対1でなくても良い。

【0034】上記の装置は、ハードウェア、ソフトウェアいずれの方法で実現されても良いし、両者を組み合わせて実現しても良い。

【0035】図5は、LAN1上に制御対象EMd124が新規に加えられた時のシステムの全体構成図である。図6は、図5のシステムにおいて、LAN1上に制御対象EMd124が新規に加えられた時に、EMd124がLC11にCPを転送し、LC11がCPの実行を開始するまでの状態と、LC11がRCb22に新規制御対象の情報を転送し、RCb22が最新のCPを転送する状態を表したシーケンス図である。

【0036】処理411で新規にシステムに参入するEMd124は、LAN1に自装置を送信先としたメッセージを送信してLAN1との接続を確認した後、LCを探すために、LAN1にブロードキャストメッセージを送信する。このブロードキャストメッセージの中にはEMd124の公開鍵暗号の公開鍵が搭載されている。処理412で、ブロードキャストメッセージを受信したLC11は、自分のアドレスと公開鍵を、前述の公開鍵を使い暗号化してEMd124に送信する。EMd124は、処理413でLC11に向けて自EMのCPのイン

ストール要求を行い、LC11は、処理414でその許可を与える。もし、許可のメッセージが返ってこない場合や不許可のメッセージが返ってきた場合には、所定の時間をおいた後、再度処理413を行う。これを所定の回数行っても処理414で許可のメッセージが返ってこない場合は、EMd124は異常状態を検知して処理を打ち切り、EMd124のシステム参入は失敗する。EMd124は、処理415で、ファイル転送プログラムを用いて自EMのCPの送信を行い、処理416で転送終了のメッセージを送信する。LC11は、処理417でこのメッセージに対して転送完了確認のメッセージを送信する。

【0037】処理417の後、LC11は処理421で、EMd124が送付してきた、EMd124の製品番号とメーカーのアドレス、及びCPのバージョンを、LC11の内部の記憶装置に格納した後、その情報をメーカーのアドレスを使ってメーカーのリモートコントロールRCa22に送信する。処理422で、RCa22は、前記の情報を受け取りその製品番号及びプログラムバージョンを調べ、自RC内に新規のEMの登録を行い、EMd124の製品サポート番号をLC11に送信する。しかしRCa22がEMd124の登録情報やその他の情報を参照し、サポートを行わないと決めた場合には、サポート不可のメッセージをLC11に送信する。LC11はこのメッセージに対して、処理を継続するかEMd124用のCPを削除するかを判断する。

【0038】処理421で、RCa22が、LC11から受け取ったメッセージの中にあったCPのバージョンが最新のものでないと判断した場合には、RCa22は処理423で、LC11に対して最新のCPをインストールする要求メッセージを送信する。処理424で、LC11からインストール許可のメッセージが返ってきた場合、RCa22は処理425で最新バージョンのCPのインストールを開始する。処理426でインストール終了のメッセージをLC11に送り、LC11は処理427で終了確認のメッセージを送って処理を終え、新規のCPにて制御を始める。

【0039】本実施例では、新規参入のEMがシステムに参入した場合について説明を行っているが、新規の制御対象に限らずリモートコントローラRCa22に格納されているCPのバージョンアップが行われた場合には、そのつどRCa22が登録しているローカルコントローラとの間に、処理423以後の処理を行うことで、制御対象は常に最新の制御プログラムがインストールされ、そのプログラムで制御されることになる。

【0040】また、これらの最新のCPのインストールを自動的に行わないように、ユーザがある制御対象のCPを設定して、新規CPのインストールの可否をディスプレイにメッセージを表示してユーザに確認することも可能である。

【0041】さらに、制御対象を制御するCPのプログラムインターフェースが公開されている場合には、ユーザは独自でCPを開発し、制御対象を制御する事が可能である。あるいは、パラメータの調節が可能なCPを用いることによって、ユーザの好みの制御を行わせることも可能となる。

【0042】なお図6の手順は、コネクション型、コネクションレス型のいずれの通信形態で実現されても良いし、両者を組み合わせて実現しても良い。また、通信メッセージの送達保証や伝送帯域の確保は、EMd124、LC11、RCa22のそれぞれの通信管理モジュールにて行っている、図5のシーケンス図では、その処理に関しては省略している。また各装置間のメッセージは、通信の初期段階にお互いの公開鍵をメッセージに送付することにより、それ以後の通信ではメッセージレベルでの暗号処理が施されている。

【0043】(実施例2)図7は、EMa121に障害が発生した状態のシステム構成図を示している。なお、本実施例における通信手段、および制御の方法に関しては、実施例1の方式に準ずるものとする。

【0044】図8は、LC11がEMa121の制御を行っている過程で障害を検知する手順を示すシーケンス図である。処理431、432、433、434では、LC11がLAN1を介してセンサ情報、及び制御情報の送受信を行い、EMa121が制御を行う過程を示している。処理435において、LC11で実行中のEMa121用CPは処理431、432、433、434で扱った情報を検証し、異常状態の検出を行う。処理435にて異常状態を検知したLC11のEMa121用のCPは処理436に対してEMa121に故障検知の依頼メッセージを送信する。EMa121は、処理437で自EM内部の故障検知探索を行い、処理438で異常の有無をLC11に知らせる。

【0045】図9は、図8の処理438で異常の有無をLC11に知らせた後、あるいはEMa121が自律的に図3の制御本体部1212において、故障及び予期せぬ停止を検知した場合、この障害をLC11のEMa121用のCPに報告し、ユーザに障害情報を示す手順を示すシーケンス図である。処理441で障害を検知したEMa121は、処理442で障害発生をLC11に送信する。このメッセージを受け取ったLC11のEMa121用のCPは、処理443でEMa121に障害情報の問い合わせを行う。このメッセージを受け取ったEMa121は、処理444で障害番号をLC11のEMa121用のCPに通知する。この後、LC11は処理445で、送られてきた障害番号を検索キーとしてCPのデータから障害情報を検索し、処理446でこれをLC11のユーザインターフェースを使ってユーザに知らせ、対策を表示する。ユーザに通知する方式としては、画像、音声など手段は問わない。

【0046】図10は、LC11で対処できない障害を、WANに接続されたローカルコントローラRCa21から直接、障害診断を行う手順を示すシーケンス図である。

【0047】処理451で障害を発見したEMa121は、処理452でLC11に障害発生の通知メッセージの送信を行う。このメッセージを受け取ったLC11のEMa121用のCPは、処理453で障害状況を問い合わせるメッセージを送信する。障害の原因が判明できなかったEMa121は、処理454で障害原因不明のメッセージをLC11のEMa121用のCPに送信する。LC11のEMa121用のCPはすでにプログラム内部に登録されているEMa121の製品番号とメーカーのアドレス検索し、処理455でそのアドレスを用いてRCa21に対してリモートテストを要求するメッセージを送信する。メッセージにはEMd124の製品サポート番号を附加する。このメッセージを受け取ったRCa21のEMa121用のCPは、製品サポート番号をチェックした後リモートテストの準備を行い、準備が

20 終了した後、処理456でリモートテスト応答のメッセージをLC11に送信する。次にLC11のEMa121用のCPは、処理457でEMa121に対し、リモートテスト要求メッセージの送信を行う。EMa121がリモートテストを受ける準備が整った後、EMa121は処理458でリモートテスト応答メッセージをLC11のEMa121用のCPに送信する。LC11のEMa121用のCPは処理460で、リモートテスト開始メッセージをRCa21のEMa121用のCPに送信し、そのメッセージを受け取ったRCa21のEMa121用のCPは処理461でリモートテストメッセージをLC11のEMa121用のCPに送り、LC11のEMa121用のCPはそのメッセージをEMa121に転送する。処理462でEMa121は、このリモートテストメッセージに対する応答メッセージをLC11のEMa121用のCPに送り、LC11のEMa121用のCPはそのメッセージをRCa21のEMa121用のCPに転送する。同様な処理を処理463、処理464で行い、テストを終了したRCa21のEMa121用のCPは、処理465で処理が終了したことを

30 通知するメッセージをLC11のEMa121用のCPに送り処理を終了する。またLC11のEMa121用のCPも処理467でテスト終了のメッセージをEMa121に送った後に処理を終了し、同様にEMa121も処理を終了する。この段階で、EMa121の故障原因が判定され、EMa121の製造元メーカーは、保守員を派遣するなどの手配を行うか、LC11のユーザインターフェースに、故障原因の詳細を表示してユーザに修理の方法を知らせる。

40 【0048】なお上記の手順は、コネクション型、コネクションレス型のいずれの通信形態で実現されても良い

し、両者を組み合わせて実現しても良い。また、通信メッセージの送達保証や伝送帯域の確保は、EMd121、LC11、RCa21のそれぞれの通信管理モジュールにて行っていて、図8、図9、図10のシーケンス図では省略されている。また各装置間のメッセージは、通信の初期段階にお互いの公開鍵をメッセージに送付することにより、それ以後の通信ではメッセージレベルでの暗号処理が施されている。

【0049】(実施例3) 図11は、図5におけるEMd124をリモートコントローラRCa21が制御する状態を示すシーケンス図である。EMd124は、リモートコントローラRCa21から直接制御され、LC11はRCa21とEMd124間でメッセージの中継を行う。

【0050】処理471で新規にシステムに参入するEMd124は、LAN1に自装置を送信先としたメッセージを送信してLAN1との接続を確認した後、ローカルコントローラを探すために、LAN1にブロードキャストメッセージを送信する。このブロードキャストメッセージの中にはEMd124の公開鍵暗号の公開鍵が搭載されている。処理472で、ブロードキャストメッセージを受信したLC11は、自分のアドレスと公開鍵を、前述の公開鍵を使ってEMd124に送信する。EMd124は、処理473でLC11に向けて、自EMのCPのインストール要求を行い、LC11は、処理474でその許可を与える。もし、許可のメッセージが返ってこない場合や不許可のメッセージが返ってきた場合には、所定の時間をおいた後、再度処理473を行う。これを所定の回数行っても処理474で許可のメッセージが返ってこない場合は、EMd124は異常状態を検知して処理を打ち切る。EMd124は、処理475で、ファイル転送プログラムを用いてCPの送信を行い、処理476で送信終了のメッセージを送信する。LC11は、このメッセージに対して送信完了確認のメッセージを送信する。

【0051】処理477の後で、LC11のEMd124用のCPは処理478で、EMd124が送付してきた、EMd124の製品番号とメーカーのアドレス、及びCPのバージョンを、LC11の記憶媒体に格納した後、その情報をメーカーのアドレスを使ってメーカーのリモートコントローラRCa21のEMd124用のCPに送信する。処理479で、RCa21のEMd124用のCPは、前記の情報を受け取りその製品番号及びプログラムバージョンを調べ、製品の登録を行い、以後EMd124の製品サポート番号をLC11のEMd124用のCPに送信する。しかしRCa21のEMd124用のCPがEMd124の登録情報やその他の情報より、サポートを行わないと決めた場合には、サポート不可のメッセージを送信する。LC11のEMd124用のCPはこのメッセージに対して、処理を継続するかC

Pを削除するかを判断する。

【0052】次に、LC11のEMd124用のCPは制御対象EMd124がリモートコントローラRCa21のEMd124用のCPから直接制御処理を受けられるように、EMd124とRCa21の通信の仲立ちを行なう処理を行う。先ず、LC11のEMd124用のCPはすでに、そのCPで登録されているEMd124の製品番号とメーカーのアドレス検索し、処理480でそのアドレスを用いてRCa21のEMd124用のCPに對してリモート制御を要求するメッセージを送信する。メッセージにはEMd124の製品サポート番号を付加する。このメッセージを受け取ったRCa21のEMd124用のCPは、リモート制御の準備を行い、準備が終了した後、処理481でリモート制御応答をLC11のEMd124用のCPに送信する。次にLC11のEMd124用のCPは、処理482でEMd124に対し、リモート制御要求メッセージを送信する。リモート制御を行う準備が整った後、EMd124は、処理483でリモート制御応答メッセージをLC11のEMd124用のCPに送信する。LC11のEMd124用のCPは処理484で、リモート制御開始メッセージをRCa21のEMd124用のCPに送信し、そのメッセージを受け取ったRCa21のEMd124用のCPは処理485でリモート制御メッセージをLC11のEMd124用のCPに送り、LC11のEMd124用のCPはそのメッセージをEMa121に転送する。処理486でEMd124は、このリモート制御メッセージに対するセンサ情報メッセージをLC11のEMd124用のCPに送り、LC11のEMd124用のCPはそのメッセージをRCa21のEMd124用のCPに転送する。同様な処理を処理487、処理488で行い、以後リモート制御を続けることになる。

【0053】なお上記の手順は、コネクション型、コネクションレス型のいずれの通信形態で実現されても良いし、両者を組み合わせて実現しても良い。また、通信メッセージの送達保証や伝送帯域の確保は、EMd124、LC11、RCa21のそれぞれの通信管理モジュールにて行なっている。また各装置間のメッセージは、通信の初期段階にお互いの公開鍵をメッセージに送付することにより、それ以後の通信ではメッセージレベルでの暗号処理が施されている。

【0054】(実施例4) 図12は、システムの外部の機器であるモバイルコンピュータ(以下、MCと呼ぶ)31を用いて、ユーザ宅内のローカルコントローラLC11のEMc123用のCPにアクセスし、EMc123の制御を行う場合のシステムの説明図である。

【0055】MC31は、電子テキストを暗号、復号することが可能な暗号モジュールを持ち、電子メールの送受信が可能な電子メールソフトウェアをインストールし

た携帯用モバイルコンピュータであり、公衆電話回線及び、他のネットワークを経由してユーザ宅内のローカルコントローラLC11へ電子メールを送信することが可能である。ユーザ宅内のローカルコントローラLC11は赤外線発受光体を持つ赤外線通信ボードを持ち、同じく赤外線発受光体を持つ赤外線通信ボードを搭載した家庭用クーラーであるEMc123と赤外線を用いて通信が可能である。

【0056】本実施例では、モバイルコンピュータMC31を用いてユーザがユーザ宅の家庭用クーラーの予約制御を行う手順について述べる。

【0057】ユーザは、モバイルコンピュータの電子メールソフトを用いて、図13に示すようなメールを作成する。501は、LC11のエアコン用のCPのメールアドレスであり、このメールはWAN2を通じてLC11のエアコン用CPに届けられる。502は、エアコン用のCPに指令を行うためのコマンドであり、ここではエアコン用CPにエアコンEMc123の制御を行うためのフォームを送るように指示するものである。503は、この電子メールを作成しているユーザの電子署名である。この署名は502のコンテンツを電子メールを使用しているユーザの秘密鍵で暗号化したものである。

【0058】図14は、図13の502及び503のコンテンツを、LC11のエアコン用CPの公開鍵で暗号化したものである。この暗号化された電子メールを、ユーザはモバイルコンピュータの電子メールソフトを用いてLC11のエアコン用CPに送信する。次にこのメールを受け取ったLC11のエアコン用CPは、先ずエアコン用CPの秘密鍵で、メールの内容を図13に示すものに復号する。次に電子メールのFrom行に付加されたユーザアドレスを読み込み、それに対応したユーザ名をLC11のユーザ登録用のデータベースから検索する。ユーザ名の検索に成功した場合、さらにそのユーザ自身が預めLC11に登録しておいた公開鍵を用いて、図13の503のコンテンツを復号する。

【0059】復号したコンテンツと図13の502の内容が一致していた場合のみ、CPは502に書かれている命令を実行する。ここでは、ユーザにエアコンEMc123の制御を行うためのフォームをユーザに電子メールで送信する命令が書かれている。エアコン用CPがユーザに電子メールを送るときにも、前述と全く同じ手順で暗号化を行う。すなわち、先ずエアコン用CPは予約制御を行うためのテンプレートを付加し、さらにエアコン用CPの秘密鍵を用いて暗号化した電子署名をフォームの後ろに付加する。さらに、このフォームと電子署名を、LC11のユーザ登録用データベースを参照してモバイルコンピュータのユーザの公開鍵を検索し、その鍵を使って暗号化した後、これをモバイルコンピュータのユーザに送信する。図15は、CPが送信するフォームを示している。このフォームには、エアコンEMc

123の制御に必要な情報（日時、設定温度、設定湿度、設定維持時間、終了報告の有無）の項目が記載されている。さらに図16では、ユーザがそのフォームに必要な項目を記載した後のメールのコンテンツを示す。ユーザはこのメールをLC11のエアコン用CPに送信し、CPはメールの内容を解釈して、CPからLAN1を経由してEMc123の設定を行う。設定に成功した場合には、図17に示すような設定成功の報告の電子メールをユーザに転送する。失敗した場合には、その原因のレポートを付けてユーザに電子メールを送信することになる。なお、本実施例におけるこれらの電子メールのやりとりの全てで、前述の暗号化・復号化の処理を行っている。

【0060】なお、エアコン用CPの秘密鍵は、プログラム内部に組み込まれているため、ユーザが取り出すことは出来ない。またこのプログラムは立ち上げ時に、秘密鍵と公開鍵を作り出すため、同じプログラムでも起動しているマシンごとに鍵は異なるものになる。

【0061】本実施例では、電子メールを用いて遠隔から制御対象を制御する方式を示しているが、あるサービス会社がこのような制御対象の制御サービスを行うには、次のような方法を用いることで簡単に実現可能である。

【0062】先ず、LC11のユーザは、遠隔のサービス会社とサービス契約を交わした後、サービス会社のアドレスと公開鍵を登録し、サービス会社はLC11のCPの公開鍵を手に入れることによって、サービス会社からの遠隔操作のサービスを受けることが可能となる。ユーザは、ユーザの要求する制御の概要を電話やファックスあるいは電子メールでサービス会社に知らせ、サービス会社は遠隔から、ユーザ宅内の機器を制御することが可能となる。本実施例では、ユーザはエアコンの複雑なインターフェースの操作を行う必要がなくなる。

【0063】なお上記の手順は、コネクション型、コネクションレス型のいずれの通信形態で実現されても良いし、両者を組み合わせて実現しても良い。また、通信メッセージの送達保証や伝送帯域の確保は、EMc123、LC11、MC31のそれぞれの通信管理モジュールにて行っている。また各装置間のメッセージは、通信の初期段階にお互いの公開鍵をメッセージに送付することにより、それ以後の通信ではメッセージレベルでの暗号処理が施されている。

【0064】(実施例5) 図18は、EMb122の制御結果をローカルコントローラLC11が、システム外部の機器であるモバイルコンピュータMC31及び、電話機TEL41に送信する場合のシステムの説明図である。

【0065】EMb122は、超音波センサによる移動体の感知装置であり、この装置の周辺で何か物体の移動があった場合にこれを感知することができる為、構内や

家屋内への不法侵入者があった場合、これを検知することが可能である。

【0066】MC31は、電子テキストを暗号、復号することが可能な暗号モジュールを持つ電子メールの送受信が可能な携帯用モバイルコンピュータであり、公衆電話回線及び、他のネットワークを経由してユーザ宅内のパソコンであるローカルコントローラLC11から電子メールを受信することが可能である。構内あるいは家屋内のローカルコントローラLC11は通信用LANボードを持ち、構内あるいは家屋内に設置され、同じく通信用LANボードを搭載した移動体感知装置であるEMc122と10BASE-Tの通信媒体を用いて通信が可能である。

【0067】本実施例では、移動体感知装置が発したアラームを、MC31およびTEL41に転送する手順について述べる。

【0068】移動体感知装置EMb122は、移動体を検知すると直ちにLC11の移動体感知装置用CPに検知情報を付加したメッセージを送信する。この情報を受け取ったLC11の移動体感知装置用CPは、LC11のユーザがLC11に直接設定した、あるいは遠隔から電子メールを用いて設定したアドレスや電話番号に検知情報を送信する。

【0069】図19は、電子メールによって送られた検知情報の内容を示すものである。521は移動体感知装置用のCPのアドレスであり、522は送信先のユーザのアドレスである。523は、メッセージの内容とそのメッセージの要求を行ったオーナーの名前が記載されている。524では、525に示す時間に異常な物体を認識したことを示している。526では、CPが行った他のアクションを示している。ここでは所定の電話番号に、音声メッセージ付きの緊急コールを発し、セキュリティ会社へ電子メールを送ったことを示している。

【0070】音声付きメッセージは予めユーザが録音しておいた音声メッセージを、アナログ機器あるいは、電子化したファイルとして記憶媒体に格納しておき、CPが、あらかじめユーザによって登録された所定の電話番号に発し、この音声メッセージを送信する。

【0071】なお上記の手順は、コネクション型、コネクションレス型のいずれの通信形態で実現されても良いし、両者を組み合わせて実現しても良い。また、通信メッセージの送達保証や伝送帯域の確保は、EMb122、LC11、MC31のそれぞれの通信管理モジュールにて行っている。また各装置間のメッセージは、通信の初期段階にお互いの公開鍵をメッセージに送付することにより、それ以後の通信ではメッセージレベルでの暗号処理が施されている。

【0072】

【発明の効果】本発明では、被制御装置が予め自分の内部装置に自分自身を制御するプログラムを所有し、シス

テムに参入する時点でリモート制御装置に制御プログラムをインストールするので、ローカル制御装置が全ての被制御装置の制御プログラムをあらかじめ持っておく必要がなくなり、リモート制御装置の管理負荷は減る。制御プログラムのインストールは、被制御装置がシステムに参入する時点で一回だけ行えば良いので、ネットワークトラヒックが高くなると言う問題や伝送帯域を確保できないと言う問題を回避できる。このことにより、被制御装置の制御プログラムは、ユーザは被制御装置をネットワークに接続する時に自動的にリモート制御装置にインストールされ、その後はその制御プログラムによって被制御装置を操作することが可能となる。

【0073】また本発明では、被制御装置の製造元メーカーなどが制御プログラムのバージョンアップを行なった時に、製造元メーカーのリモート制御装置が、被制御装置の制御を行っているローカル制御装置にWANを介してその新規の制御プログラムをインストールするので、被制御装置は制御の方式を常に最新のものに変更することが可能である。あるいはその新規の制御プログラムの情報を、ローカルコントローラのユーザインターフェースを介してユーザに知らせることにより、ユーザは制御プログラムの選択が可能となり、また、ユーザは自分の好みの制御を被制御装置に行わせることが可能となる。

【0074】また本発明では、本発明のそれぞれの装置が暗号方式を用いることによって、各種のメッセージや制御プログラムの内容が変更されていないことが保証され、情報の送信元の装置が明らかになる。これによってシステムに無関係な装置からのメッセージやプログラムの誤送信、あるいは悪意の第三者がシステムへの不正アクセスを不可能にする。

【0075】また本発明では、ローカル制御装置、あるいはリモート制御装置が、被制御装置から直接にセンサ情報などの情報を受信し、その受信した情報を制御プログラムに入力し、制御情報を得、その得られた制御情報を被制御装置に送信する。これによって制御処理能力を持つローカル制御装置、あるいはリモート制御装置によって、被制御装置の高度な精密制御が可能となる。

【0076】また本発明では、リモート制御装置や移動体端末が、WANとローカル制御装置を介して被制御装置の制御を行うことによって、サービス会社やユーザがリモートから被制御装置の制御を行うことが可能となる。

【0077】また本発明では、被制御装置が自律的かつ定期的に保守管理情報をローカル制御装置やリモート制御装置に送信したり、あるいはローカル制御装置あるいはリモート制御装置が定期的に被制御装置に保守管理情報を送信する指令を与え、被制御装置がこれに対して保守管理情報を送信する。これによって、ローカル制御装置あるいはリモート制御装置は、被管理装置の状態を常時監視し、必要に応じてその状態をユーザに知らせるこ

とが可能となるので、ユーザが製品の異常や停止になつた時点で、初めて故障に気がつくと言う問題を回避することが可能となる。

【0078】また本発明では、ローカル制御装置が被制御情報から送られてきた情報を、ユーザによって予め決められたアドレスに送信する。これによって、遠隔地のサービス会社やユーザが、被制御装置の状態を常時確認することが可能となる。

【図面の簡単な説明】

【図1】実施例1における本発明が適用されるシステムの説明図。

【図2】実施例1における図1のローカルコントローラの説明図。

【図3】実施例1における図1の制御対象の説明図。

【図4】実施例1における図1のリモートコントローラの構成図。

【図5】実施例1における新規の制御対象参入時のシステムの全体構成図。

【図6】実施例1における最新の制御プログラムを転送する状態を示すシーケンス図。

【図7】実施例2における制御対象に障害が発した状態のシステム構成図。

【図8】実施例2における制御対象の障害を検知する手順のシーケンス図。

【図9】実施例2におけるユーザに障害情報を示す手順を示すシーケンス図。

【図10】実施例2における障害診断を行う手順を示すシーケンス図。

\* 【図11】実施例3におけるリモート制御の手順を示すシーケンス図。

【図12】実施例4におけるシステム全体の構成図。

【図13】実施例4における電子メールの説明図。

【図14】実施例4における電子メールを暗号化した説明図。

【図15】実施例4における制御フォームを記した電子メールの説明図。

【図16】実施例4における制御フォームにユーザが記入した電子メールの説明図。

【図17】実施例4における制御結果のレポートを記入した電子メールの説明図。

【図18】実施例5における制御対象が制御結果を送信する状態を示すシステムの説明図。

【図19】実施例5における制御対象の検知情報の内容を示す電子メールの説明図。

【符号の説明】

LAN…ローカルエリアネットワーク、

WAN…ワイドエリアネットワーク、

LC…ローカルコントローラ、

EM…制御対象、

RC…リモートコントローラ、

PTA…プログラム転送エージェント、

MTA…メッセージ転送エージェント、

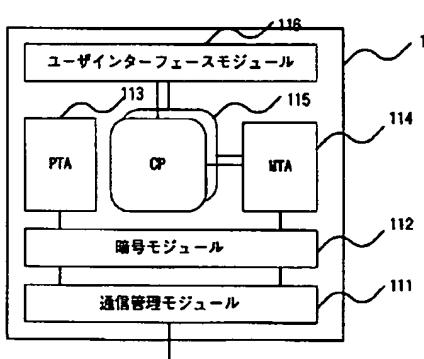
CP…制御プログラム、

MC…モバイルコンピュータ、

TEL…電話機。

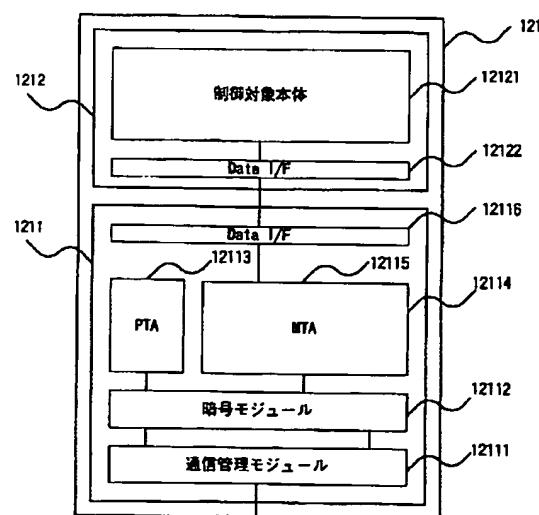
【図2】

図 2



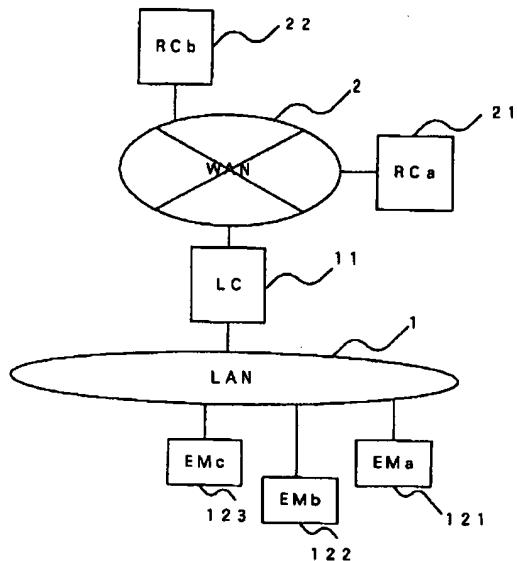
【図3】

図 3



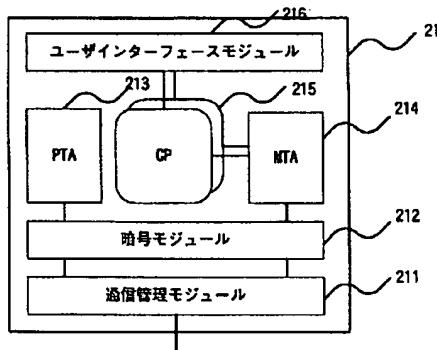
【図1】

図1



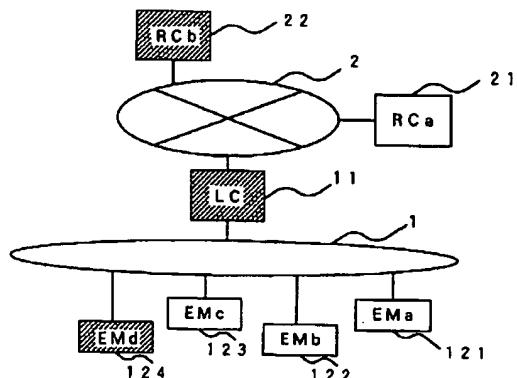
【図4】

図4

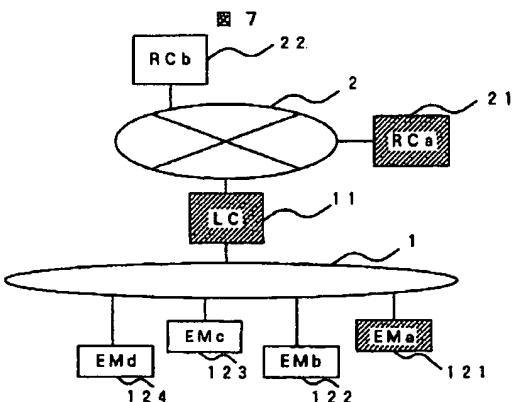


【図5】

図5



【図7】



【図13】

図13

To: aircord@LC11.homeauto.or.jp  
Subject:  
send for~  
—BEGIN CODE SIGNATURE—  
a)afidjgidiacufel|f1adffjh|f1fe  
oiqith  
—END CODE SIGNATURE—

【図14】

図14

To: aircord@LC11.homeauto.or.jp  
Subject:  
—BEGIN CODE MESSAGE—  
6af4-ha+9817gas4|9w6u009us8lh  
w68th9879-a87h+n#lrb87h9+8ery  
-3e897h98s1+et/7a84gh  
—END CODE MESSAGE—

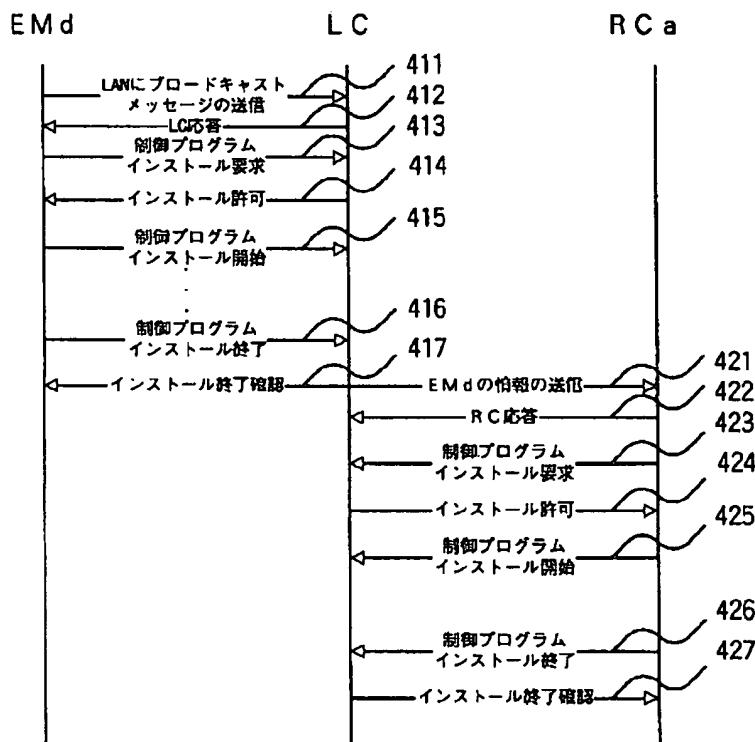
【図15】

図15

From:aircord@LC11.homeauto.or.jp  
To:cbaied@sd1.hitachi.co.jp  
date:  
start time:  
capture:  
humidity:  
alive time(<5 hours)  
end of report(read or not)

【図6】

図 6



【図16】

図 16

```

From:ebata@sd1.hitachi.co.jp
To:aircon@LC11.hccauto.or.jp

date: 96/07/20
start time: 18:00
tempature: 24
humidity: 50
alive time(<5 hours)
end of report(need or not) n

```

【図17】

図 17

```

From:aircon@LC11.hccauto.or.jp
To:ebata@sd1.hitachi.co.jp

Accepted your order as follow

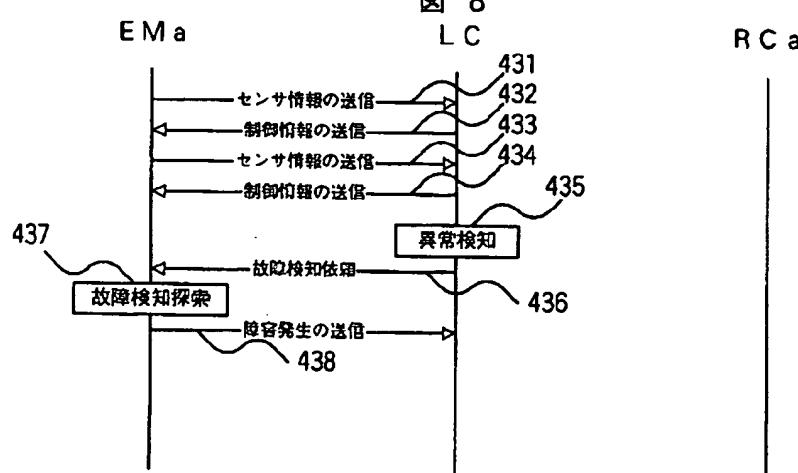
date: 96/07/20
start time: 18:00
tempature: 24
humidity: 50
alive time(<5 hours)
end of report(need or not) n

Thank you.

```

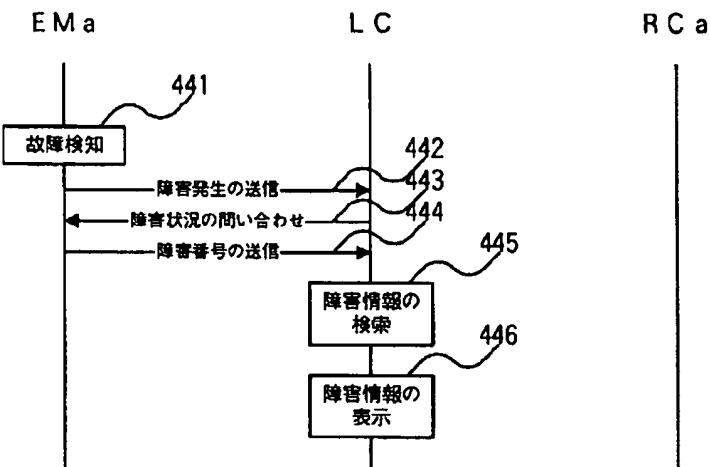
【図8】

図 8

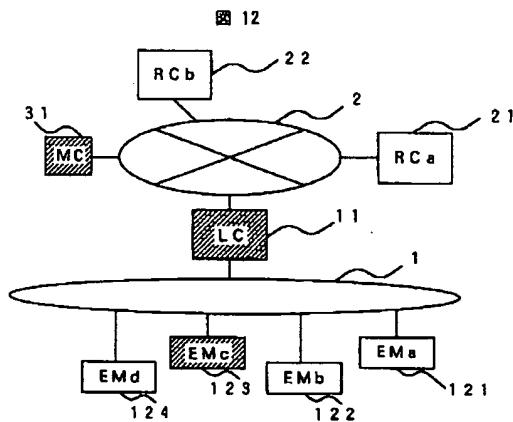


【図9】

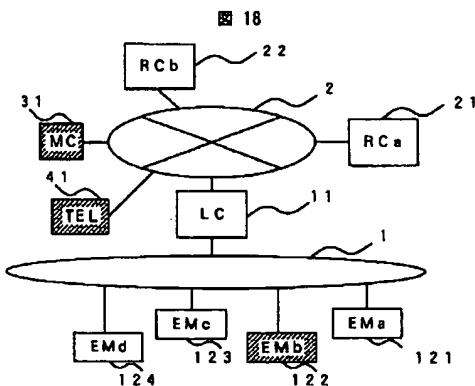
図 9



【図12】



【図18】



【図19】

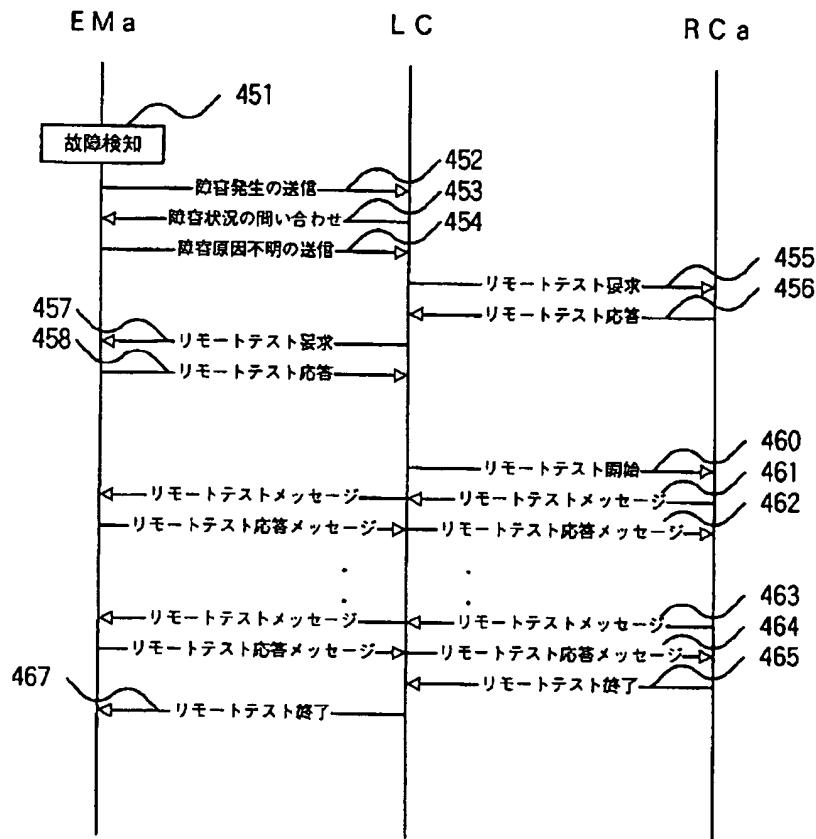
図19

```

521 From:sonic-sensor@LC1.homeauto.or.jp
522 To:obata@edl.hitachi.co.jp
523 I did an action I was get order by
      obata(obata@edl.hitachi.co.jp) as follow.
524
525 Action: abnormal object appeared,
      Date/Time:1996/07/22 18:45:03
526
      The others : Call 044-988-7935 with Emergency voice message
      Co-Bell info@axcom.security.or.jp
  
```

【図10】

図 10



【図11】

図11

